IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant: Liqun Chen *et al.*	)	On Appeal to the Board of Appeals
Patent Application No.: 09/913,454	)	
Filed: 08/14/2001	)	Group Art Unit: 2137
	)	Examiner: Nguyen, Minh Dieu T
For: "Protection of the Configuration ..."	)	
	)	Date: April 08, 2008

BRIEF ON APPEAL

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from the final Office Action, dated October 15, 2007, for the above identified patent application. Appellants submit that this Appeal Brief is being timely filed, because the Notice of Appeal was filed on January 8, 2008. Please charge the Appeal Brief fee of $510.00 to deposit account no. 08-2025.

REAL PARTY IN INTEREST

The real party in interest to the present application is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

RELATED APPEALS AND INTERFERENCES

Appellants submit that there are no other prior and pending appeals, interferences or judicial proceedings which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

STATUS OF CLAIMS

Claims 44-53 and 57-67 are currently pending. Claims 44-53 and 57-67 stand rejected, are the subject of this Appeal, and are reproduced in the accompanying Claims Appendix.

STATUS OF AMENDMENTS

An Amendment after Final Rejection has been filed on March 06, 2008. In that amendment, claim 57 has been amended to address the claim objections from the Examiner as noted on page 4, section 5, of the final Office Action.

SUMMARY OF CLAIMED SUBJECT MATTER

The invention described and claimed in the present application relates to the protection of configuration of modules in a computing apparatus (p. 1, ll. 3-4).

Claim 44 of the present disclosure is directed to a method of protecting from modification computer apparatus (10) comprising a plurality of functional modules (15), wherein the computer apparatus contains or is in communication with a trusted device (24) adapted to respond to a user in a trusted manner, the method comprising: storing a module configuration of the computer apparatus providing an identification of each functional module in the computer apparatus (p. 18, second full paragraph – p. 19, third full paragraph); the trusted device performing a cryptographic identification process for modules with a cryptographic identity to identify them and thereby determine an actual module configuration (Fig. 4, p. 11, l. 1 to p. 13, l. 8); the trusted device comparing the actual module configuration against the stored module configuration (p. 19, third full paragraph); and the trusted device inhibiting function of the computer apparatus while

the actual module configuration does not satisfactorily match the stored module configuration (Fig. 5, p. 13, l. 26 to p. 15).

Claim 52 of the present disclosure is directed to a computer apparatus (10) adapted for protection against modification, the computer apparatus comprising a plurality of functional modules (15), one of said modules being a trusted device (24) adapted to respond to a user in a trusted manner, the computer apparatus having a module configuration providing an identification of each functional module in the computer apparatus (p. 18, second full paragraph – p. 19, third full paragraph), wherein the trusted device is adapted to compare a module configuration of the computer apparatus against a stored module configuration by performing a cryptographic identification process for modules with a cryptographic identity to determine an actual module configuration and to compare the actual module configuration against the stored module configuration (Fig. 5, p. 13, l. 26 to p. 15).

Claim 57 of the present disclosure is directed to a method of protecting from modification computer apparatus (10) comprising a plurality of functional modules (15) by monitoring the configuration of functional modules within the computer apparatus, the method comprising: storing a module configuration of the computer apparatus, the module configuration being an identification of each functional module in the computer apparatus as validly formed, on a security token removably attachable to the computer apparatus (p. 5, third full paragraph of "Description of the Preferred Embodiment," p. 9, third full paragraph, p. 19, first full paragraph); and checking an actual module configuration against the stored module configuration (p. 19, third full paragraph); wherein the computer apparatus contains or is in communication with a trusted device adapted to respond to a user in a trusted manner and the trusted device inhibits function of the computer apparatus if the actual module configuration does not satisfactorily match the stored module configuration. (Figs 4-6, p. 13, l. 26 to p. 15, p. 16, l. 1 to p.18, l. 4).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Issue 1: Whether Claims 44-47, 50, 52-53 and 58 are patentable under 35 U.S.C. 103(a) in view of Probst, U.S. Patent No. 5,982,899, (hereinafter, "Probst") and further in view of Selitrennikoff, U.S. Patent No. 6,209,089, (hereinafter, "Selitrennikoff")?

Issue 2: Whether Claims 48-49, 57-63 are patentable under 35 U.S.C. 103(a) in view of Probst, Selitrennikoff and further in view of Herzi, U.S. Patent No. 6,353,885, (hereinafter, "Herzi")?

Issue 3: Whether Claims 51 and 64 are patentable under 35 U.S.C. 103(a) in view of Probst, Selitrennikoff, Herzi and further in view of Muftic, U.S. Patent No. 5,943,423, (hereinafter, "Muftic")?

Issue 4: Whether Claims 65-67 are patentable under 35 U.S.C. 103(a) in view of Probst, Selitrennikoff, and further in view of Micali, U.S. Patent No. 5,499,296, (hereinafter, "Micali")?

ARGUMENT

Issue 1: Whether Claims 44-47, 50, 52-53 and 58 are patentable under 35 U.S.C. 103(a) in view of Probst, U.S. Patent No. 5,982,899, (hereinafter, "Probst") and further in view of Selitrennikoff, U.S. Patent No. 6,209,089, (hereinafter, "Selitrennikoff")?

In the final Office Action of October 15, 2007, the Examiner rejects Claims 44-47, 50, 52-53 and 58 under 35 U.S.C. 103(a) as being obvious in view of Probst and Selitrennikoff. Appellants respectfully disagree.

I. Appellants submit that a *prima facie* case of obviousness has **not** been established because the Examiner has failed to show that Probst and

Selitrennikoff teach each and every element as claimed in the present application. In particular:

Claim 44

A. Appellants submit that the Examiner has not shown that Probst and Selitrennikoff disclose, suggest or teach, *inter alia*, the following features recited by Claim 44 of the present application:

> "the **trusted device** comparing the actual module configuration against the stored module configuration" (emphasis added)

According to Probst, Probst's processor 31 compares the encrypted configuration data and the actual configuration data (c. 7, ll. 36-39 of Probst). Contrary to Probst, "trusted device" of Claim 44 compares "the actual module configuration against the stored module configuration."

According to claim 44, the "trusted device" is "adapted to respond to a user in a trusted manner." Appellants submit that Probst does not disclose that the processor 31 is able to respond to a user in a trusted manner because after a thorough review of Probst, Probst is found silent regarding the processor 31 being able to respond to a user in a trusted manner. The Examiner cites column 3, lines 8-30 of Probst as allegedly teaching the limitation. This paragraph actually teaches:

> Data which is expressive of the configuration of a computer system advantageously is encrypted during manufacturing of the computer system. This is done by using an identifier which is assigned to the computer system or a component thereof during manufacturing. The private key which is used for the encryption of the encoded data is only known to the manufacturer of the computer system.
>
> The RSA cryptosystem preferably is used for encryption of the encoded data (cf. R. L. Rivest, A. Shamir and L. Adleman "A Method for Obtaining Digital Signatures and

> Public-Key Cryptosystems", Communications of the ACM, February 1978, Vol. 21, No. 2). For encoding the data by means of the identifier, the identifier can for example simply be added to the data. For decoding the identifier is subtracted later on from the encoded data. Also the DES method can be used whereby the identifier of the computer system is employed as a secret key (cf. Cheryl Ajluni, "Security Techniques Ensure Privacy", Electronic Design, Apr. 17, 1995, page 98).
>
> The encrypted data can be stored in any kind of storage device of the computer system, for example on an EPROM or on a diskette.

As the reader will appreciate, there is nothing in this passage that could be understood by the skilled person as teaching a trusted device "adapted to respond to a user in a trusted manner."

Because Probst's processor 31 is not described as being adapted to respond to a user in a trusted manner, Probst does not teach, disclose or suggest the "trusted device" as recited in Claim 44. Hence, Claim 44 is patentable over Probst and the Examiner's rejection should be overturned on appeal.

B. Appellants submit that the Examiner has not shown that Probst and Selitrennikoff disclose, suggest or teach, *inter alia*, the following features recited by Claim 44 of the present application:

> "the **trusted device comparing** the actual module configuration against the stored module configuration;
> the **trusted device inhibiting function of the computer** apparatus while the actual module configuration does not satisfactorily match the stored module configuration." (emphasis added)

Although the Examiner asserts that Probst inhibits function of the computer (p. 5, last 3 lines of the final Office Action), he is silent on which of Probst's components actually inhibits function of the computer.

According to Claim 44, the "trusted device" compares "the actual module configuration against the stored module configuration" and inhibits "function of the computer apparatus." As shown above, Probst's processor 31 compares the encrypted configuration data and the actual configuration data (c. 7, ll. 36-39 of Probst). Appellants respectfully submit that the Examiner has been unable to "designate as nearly as practicable" where Probst discloses that the processor 31 inhibits the function of the computer.

According to Probst, the computer system is either shut down or booting procedure is interrupted when comparison performed by the processor 31 reveals a mismatch (c.7, ll. 49-60 of Probst). However, Probst does not teach, disclose or suggest that the processor 31 inhibits "function of the computer apparatus" as recited in Claim 44. At best, processor 31 may be considered as inhibiting "function of the computer apparatus" but not as "the trusted device inhibiting function of the computer."

Because Probst's processor 31 does not inhibit "function of the computer apparatus" as recited in Claim 44, Claim 44 is patentable over Probst and rejection of claim 44 should be overturned on appeal.

C. Appellants submit that the Examiner has <u>not</u> shown that Probst and Selitrennikoff disclose, suggest or teach, *inter alia*, the following features recited by Claim 44 of the present application:

> "the **trusted device performing a cryptographic identification process** for modules with a cryptographic identity to identify them and thereby determine an actual module configuration" (emphasis added)

The Examiner concedes that Probst does not disclose "performing a cryptographic identification process for modules with a cryptographic identity" to "determine an actual module configuration" as recited in Claim 44. The Examiner alleges that the concept of a cryptographic identification process with a cryptographic identity is performed by

Probst steps 7-11 when determining the stored module configuration (p. 5, Section 7a, ll. 9-11 of the final Office Action), and that this concept can be implemented for determining actual module configuration (p. 5, Section 7a, ll. 11-13 of the final Office Action). Appellants respectfully disagree with the Examiner's allegation.

According to Probst's steps 7-11, Probst obtains encoded data from an EPROM, decrypts it with a public key and decodes it with an identifier (column 5, ll. 40-50 of Probst). However, Appellants submit that the actual configuration data **is stored in unencrypted form** (column 7, ll. 37-39 of Probst). Consequently, decrypting data that is not encrypted would lead to unpredictable results.

Appellants submit that Probst teaches away from "performing a cryptographic identification process for modules with a cryptographic identity" to "determine an actual module configuration" as recited in Claim 44, because Probst specifically teaches that the actual configuration data **is stored in unencrypted form** and therefore would not require decryption as performed by steps 7-11. Because Probst teaches away from "performing a cryptographic identification process for modules with a cryptographic identity" to "determine an actual module configuration" as recited in Claim 44, the Examiner's allegation that "the concept of a cryptographic identification process with a cryptographic identity is performed by Probst steps 7-11 when determining the stored module configuration, and that this concept can be implemented for determining actual module configuration" is incorrect and for that reason, Appellants submit that Claim 44 is patentable over Probst and the rejection should be overturned on appeal.

Appellants respond to the Examiner's Response to Arguments on pp. 2-4 of the Office Action as follows.

(i) On page 2 of the final Office Action, the Examiner has disagreed with the Appellants' arguments that Probst compares the encrypted configuration data and the actual configuration data, not "the actual module configuration against the stored module configuration," as recited in claim 44. The Examiner has cited column 3, lines 43-45, of

Probst, which states, "Once the encrypted data is stored on a storage device of the computer system, the encrypted data is used for verifying the configuration." However, Appellants respectfully submit that this teaching is devoid of disclosing an actual module configuration, or a stored module configuration, and specifically, "the trusted device comparing the actual module configuration against the stored module configuration," as recited in claim 1. This is because the teaching "Once the encrypted data is stored on a storage device of the computer system, the encrypted data is used for verifying the configuration" of Probst is not the same as the presently claimed "the trusted device comparing the actual module configuration against the stored module configuration" because the cited storage device is not the same as the claimed "trusted device," and the cited encrypted data is not the same as the claimed "stored module configuration." Therefore, Appellants submit that the disagreement of the Examiner should be overturned on appeal.

(ii) The Examiner seems to have misread *Kropa* on page 3 of the final Office Action (first paragraph). *Kropa v. Robie*, 187 F.2d at 152, 88 USPQ2d at 480-81 (preamble is not a limitation where claim is directed to a product and the preamble merely recites a property inherent in an old product defined by the remainder of the claim). Here, claim 44 is a method claim and the limitation "adapted to respond to a user in a trusted manner" is not inherent in an old product or method defined by the remainder of the claim. The Examiner is respectfully reminded of MPEP 2111.02 [I], on Effect of Preamble, which states in part:

> Any terminology in the preamble that limits the structure of the claimed invention must be treated as a claim limitation. See, e.g., *Corning Glass Works v. Sumitomo Elec. U.S.A., Inc.*, 868 F.2d 1251, 1257, 9 USPQ2d 1962, 1966 (Fed. Cir. 1989) (The determination of whether preamble recitations are structural limitations can be resolved only on review of the entirety of the application "to gain an understanding of what the inventors actually invented and intended to encompass by the claim."); *Pac-Tec Inc. v. Amerace Corp.*, 903 F.2d 796, 801, 14 USPQ2d 1871, 1876 (Fed. Cir. 1990)

> (determining that preamble language that constitutes a structural limitation is actually part of the claimed invention). See also *In re Stencel*, 828 F.2d 751, 4 USPQ2d 1071 (Fed. Cir. 1987). (The claim at issue was directed to a driver for setting a joint of a threaded collar; however, the body of the claim did not directly include the structure of the collar as part of the claimed article. The examiner did not consider the preamble, which did set forth the structure of the collar, as limiting the claim. The court found that the collar structure could not be ignored. While the claim was not directly limited to the collar, the collar structure recited in the preamble did limit the structure of the driver. "[T]he framework - the teachings of the prior art - against which patentability is measured is not all drivers broadly, but drivers suitable for use in combination with this collar, for the claims are so limited." Id. at 1073, 828 F.2d at 754.).

In the instant case, the preamble sets forth "a method of protecting from modification" which limits the claim. A terminology in the preamble that limits the structure of the claimed invention must be treated as a claim limitation. Accordingly, Appellants respectfully submit that the feature "trusted device adapted to respond to a user in a trusted manner" be considered on appeal.

(iii) On page 3, second full paragraph, of the final Office Action, the Examiner has rejected the Appellants' argument that Probst does not teach, disclose or suggest that the processor 31 inhibits "function of the computer apparatus" as recited in Claim 44. The Examiner has cited column 4, lines 24-25, of Probst stating "If the data and the configuration data do not match it is possible not to enable or to disable the entire system," and column 7, lines 49-53, of Probst stating "If the comparison carried out by the service processor 31 reveals that there is no perfect match this can cause the interruption of the booting procedure so that the entire computer system is disabled." Appellants respectfully submit that the "trusted device" of appellants' claim 44 is distinct from the processor 31 of Probst because Probst is silent regarding the processor 31 being able to respond to a user in a trusted manner.

Therefore, Appellants submit that the disagreement of the Examiner be overturned on appeal.

(iv) Regarding the Examiner's comments in the third paragraph beginning on page 3 of the final Office Action, reproduced below:

> ... it is well known in the data communication world that encrypting is used to protect data for security reason that is disclosed by Probst (Fig. 1). For that same reason, the actual configuration data can be protected by implementing the same concept that is used for the stored encrypted configuration data as taught by Probst. The previous office action asserted Fig. 2, elements 7-11 to illustrate how the stored encrypted module configuration is derived by inversing the encryption process, it is well-understood that one cannot decrypt data that is not encrypted as submitted in the Remarks.

Appellants respectfully submit that the reasons Appellants cited in the previous response of record still stand because Probst teaches away from "performing a cryptographic identification process for modules with a cryptographic identity" to "determine an actual module configuration" as recited in Claim 44, because Probst specifically teaches that the actual configuration data is stored in unencrypted form and therefore would not require decryption as performed by steps 7-11 of Probst's Fig. 2.

The Examiner has cited "Alternatively--instead of decoding the decrypted data--it is also possible to encode the configuration data which is stored in an encoded form in the computer system and to compare the encoded data with the encoded configuration data" from column 4, lines 19-23 of Probst. But this text is still devoid of "the trusted device performing a cryptographic identification process for modules with a cryptographic identity to identify them and thereby determine an actual module configuration" as recited in Appellants' claim 44 because this passage of Probst discusses that the actual configuration data is stored in unencrypted form, not "performing a cryptographic identification process for modules with a cryptographic identity" to "determine an actual module configuration" as recited in Claim 44. Stated

differently, Probst does not teach "performing a cryptographic identification process for modules with a cryptographic identity" to "determine an actual module configuration" because, as shown in Figure 8 of the application and accompanying description on page 20 of the application, a cryptographic identification process involves a challenge/response routine and if an authentic response is received, a secure process is executed. Accordingly, column 4, lines 19-23, of Probst is devoid of "the trusted device performing a cryptographic identification process for modules with a cryptographic identity to identify them and thereby determine an actual module configuration." In this regard, Appellants respectfully submit that the "cryptographic identification process" does not have a commonly accepted meaning. Therefore, Appellants request the reader to look to the specification to arrive at the commonly accepted meaning of the "cryptographic identification process."

Therefore, Appellants submit that the disagreement of the Examiner be overturned on appeal.

Claims 45-47 and 50

Claims 45-47 and 50, at least based on their dependency on Claim 44, are also patentable over Probst and Selitrennikoff and their rejection should be overturned on appeal.

Claim 52

Appellants submit that, for the reasons stated above for Claim 44, Probst and Selitrennikoff do not teach, disclose or suggest "a **trusted device adapted to respond** to a user in a trusted manner," "**trusted device is adapted to compare** a module configuration of the computer apparatus against a stored module configuration," and "the trusted device ... performing a cryptographic identification process for modules with a cryptographic identity to determine an actual module configuration" (emphasis added) as recited in Claim 52. Hence, Claim 52 is patentable over Probst and Selitrennikoff and the Examiner's rejection should be overturned on appeal. Claim 53, at least based

on its dependency on Claim 52, is also patentable over Probst and Selitrennikoff and its rejection should be overturned on appeal.

Issue 2: Whether Claims 48-49, and 57-63 are patentable under 35 U.S.C. 103(a) in view of Probst, Selitrennikoff, and further in view of Herzi, U.S. Patent No. 6,353,885, (hereinafter, "Herzi")?

In the final Office Action of October 15, 2007, the Examiner rejects Claims 48-49, and 57-63 under 35 U.S.C. 103(a) as being obvious in view of Probst, Selitrennikoff and Herzi. Appellants respectfully disagree.

Appellants submit that a *prima facie* case of obviousness has not been established because the Examiner has failed to show that Probst, Selitrennikoff and Herzi teach each and every element as claimed in the present application. In particular:

Claims 48-49

The Examiner has rejected claims 48 and 49 over Probst in view of Selitrennikoff and further in view of Herzi. Appellants respectfully traverse.

Claim 48 recites "A method as claimed in claim 47, wherein the stored module configuration is stored in a security token." The Examiner concedes on page 7 of the Office Action that Probst and Selitrennikoff are silent on the capability of the stored module configuration being stored on a security token and wherein the security token is a smart card. However, the Examiner cites column 3, lines 54-57 and 5-13, of Herzi for a disclosure of the security token and the smart card. Appellants respectfully disagree because Herzi does not disclose a security token..

Herzi discloses a computer system having a capability for implementing BIOS level configuration settings which includes at least one processor, at least one memory, basic input output system (BIOS) firmware, and at least one BIOS configurable device. The at

least one memory includes operating system code. The BIOS firmware includes a smart card BIOS level setting support feature. The BIOS configurable device is subject to being configured by the at least one processor in response to a prescribed smart card actuation of the smart card BIOS level setting support feature prior to a booting of the operating system code. (Herzi Abstract).

Appellants submit that Herzi is oriented towards an improved system and method for providing BIOS-level user configuration in a multi-user computer system environment. (Column 2, lines 21-23 of Herzi). Herzi is not oriented towards encryption or security. As a result, Herzi does not teach, disclose, or suggest a "security token." More specifically, Herzi does not teach, disclose, or suggest "the stored module configuration is stored in a security token," as recited in claim 48. (Column 6, lines 5-7 of Herzi).

Moreover, Herzi teaches away from encryption because Herzi discloses, "The PIN data is already secure on be smart card. The smart card is thus more convenient than having to use some form of encryption for saving the BIOS level settings."

Accordingly, Appellants submit that claim 48 is patentably unobvious over Probst in view of Selitrennikoff and further in view of Herzi because does not teach, disclose, or suggest "the stored module configuration is stored in a security token," as recited in claim 48, and because Herzi "teaches away" from encryption. Therefore, Appellants request that the rejection of claim 48 be overturned on appeal. Further, claim 49, depending from claim 48, is in condition for allowance at least for the reasons stated above. Therefore, Appellants request that the rejection of claim 49 be overturned on appeal.

Claim 57

Appellants submit that, at least for the reasons stated above for Claim 44, Probst, Selitrennikoff and Herzi do not teach, disclose or suggest "wherein the computer apparatus contains or is in communication with a **trusted device adapted to respond**

to a user in a trusted manner and the **trusted device inhibits function of the computer apparatus** if the actual module configuration does not satisfactorily match the stored module configuration" (emphasis added) as recited in amended Claim 57. Hence, Claim 57 is patentable over Probst, Selitrennikoff and Herzi and the Examiner's rejection should be overturned on appeal. Claims 58-63, at least based on their dependency on Claim 57, are also patentable over Probst, Selitrennikoff and Herzi, and their rejection should be overturned on appeal.

On page 8 of the final Office Action, in the first paragraph, the Examiner has referred to passages already cited in the previous Office Action (column 3, lines 1-3; column 3, lines 8-30; column 4, lines 11-14; column 4, lines 24-25). Appellants have already argued that such passages do not teach or suggest the Appellants' claim 44. The Examiner has referred to FIG. 4 of Probst which is merely a schematic block diagram of a computer system which may be utilized to implement the method and system of Probst. FIG. 4 does not teach, disclose or suggest "wherein the computer apparatus contains or is in communication with a trusted device adapted to respond to a user in a trusted manner and the trusted device inhibits function of the computer apparatus if the actual module configuration does not satisfactorily match the stored module configuration," recited in claim 57. Therefore, Appellants respectfully request that the rejection of claim 57 be overturned on appeal.

Issue 3: Whether Claims 51 and 64 are patentable under 35 U.S.C. 103(a) in view of Probst, Selitrennikoff, Herzi and further in view of Muftic, U.S. Patent No. 5,943,423, (hereinafter, "Muftic")?

In the final Office Action of October 15, 2007, the Examiner rejects Claims 51 and 64 under 35 U.S.C. 103(a) as being obvious in view of Probst, Selitrennikoff, Herzi and Muftic. Appellants respectfully disagree.

Appellants submit that Claims 51 and 64, at least based on their dependency on Claims 44 and 57, respectively, are believed to be patentable over Probst, Selitrennikoff, Herzi and Muftic, because there is no prima facie 35 USC 103(a) case based on Probst and Selitrennikoff, as shown above, and because the Examiner has not shown where Muftic discloses, teaches or suggests the features not found in Probst, Selitrennikoff, and Herzi discussed above. Therefore, the rejection of claims 51 and 64 should be overturned on appeal.

Issue 4: Whether Claims 65-67 are patentable under 35 U.S.C. 103(a) in view of Probst, Selitrennikoff, and further in view of Micali, U.S. Patent No. 5,499,296, (hereinafter, "Micali")?

In the final Office Action of October 15, 2007, the Examiner rejects Claims 65-67 under 35 U.S.C. 103(a) as being obvious in view of Probst, Selitrennikoff, and Micali. Appellants respectfully disagree.

Claim 65 depends from claim 44, claim 66 depends from claim 52, and claim 67 depends from claim 57.

In the text cited by the Examiner (Column 4, lines 21-33 and 60-62), Micali merely describes that the encryptor and the digitizer are coupled either physically, logically or through non-tamperable software to guarantee that a given ciphertext is the encryption, generated by the encryptor, of an output generated by the digitizer, and a technique to physically couple the digitizer and the encryptor through placement of these devices in the same tamper-proof area of the secure device. Therefore, Micali does not bridge the gap left by Probst and Selitrennikoff because Micali makes no mention of "the trusted device comparing the actual module configuration against the stored module configuration," as recited in claim 44, "the trusted device is adapted to compare ... the

actual module configuration against the stored module configuration," as recited in claim 52, or the "trusted device inhibits function of the computer apparatus if the actual module configuration does not satisfactorily match the stored module configuration" as recited in claim 57.

Further, Appellants submit that Claims 65-67, at least based on their dependency on Claims 44, 52, and 57, respectively, are also patentable over Probst, Selitrennikoff, and Micali, because there is no prima facie 35 USC 103(a) case based on Probst and Selitrennikoff, as shown above, and because the Examiner has not shown where Micali discloses, teaches or suggests the features not found in Probst and Selitrennikoff. Therefore, the rejection of claims 65-67 should be overturned on appeal.

* * *

Conclusion

For the extensive reasons advanced above, Appellants respectfully contend that each pending claim is patentable. Therefore, reversal of all rejections and objections and allowance of this application is courteously solicited.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2025. In particular, if this Appeal Brief is not timely filed, the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136(a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2025.

I hereby certify that this correspondence is being transmitted to the United States Patent and Trademark Office via electronic filing on

April 08, 2008
(Date of Mailing)

Krista Celentano
(Name of Person Mailing)

/Krista Celentano/
(Signature)

April 08, 2008
(Date)

Respectfully submitted,

/Amit Singh 54,451/

Amit Singh
Attorney for Appellants
Reg. No. 54,451
LADAS & PARRY LLP
5670 Wilshire Boulevard, Suite 2100
Los Angeles, CA 90036
(323) 934-2300

Enclosures:
Claims appendix;
Evidence appendix; and
Related Proceedings appendix.

Amendments to the Claims

This listing of the claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1-43. (Cancelled)

44. A method of protecting from modification computer apparatus comprising a plurality of functional modules, wherein the computer apparatus contains or is in communication with a trusted device adapted to respond to a user in a trusted manner, the method comprising:

storing a module configuration of the computer apparatus providing an identification of each functional module in the computer apparatus;

the trusted device performing a cryptographic identification process for modules with a cryptographic identity to identify them and thereby determine an actual module configuration;

the trusted device comparing the actual module configuration against the stored module configuration; and

the trusted device inhibiting function of the computer apparatus while the actual module configuration does not satisfactorily match the stored module configuration.

45. A method as claimed in claim 44, wherein the stored module configuration is held separately from the computing apparatus.

46. A method as claimed in claim 44, wherein the stored module configuration is stored such that it is accessible only by a cryptographic authentication process.

47. A method as claimed in claim 44, wherein the trusted device is adapted to communicate securely with the stored module configuration.

48. A method as claimed in claim 47, wherein the stored module configuration is stored in a security token.

49. A method as claimed in claim 48, wherein the security token is a smart card.

50. A method as claimed in claim 44, wherein the step of checking of the actual module configuration comprises a cryptographic identification process for modules with a cryptographic identity.

51. A method as claimed in claim 48, wherein a stored module configuration is held by a remote module validation authority and the remote validation authority provides a service allowing a replacement security token to be provided if a security token is lost or stolen.

52. Computer apparatus adapted for protection against modification, the computer apparatus comprising a plurality of functional modules, one of said modules being a trusted device adapted to respond to a user in a trusted manner, the computer apparatus having a module configuration providing an identification of each functional module in the computer apparatus, wherein the trusted device is adapted to compare a module configuration of the computer apparatus against a stored module configuration by performing a cryptographic identification process for modules with a cryptographic identity to determine an actual module configuration and to compare the actual module configuration against the stored module configuration, wherein function of the computer apparatus is inhibited while the actual module configuration does not satisfactorily match the stored module configuration.

53. Computer apparatus as claimed in claim 52, wherein the stored module configuration is held separately from the computing apparatus and wherein the computer apparatus is adapted to obtain the stored module configuration by a cryptographic authentication process.

54-56. (canceled)

57. A method of protecting from modification computer apparatus comprising a plurality of functional modules by monitoring the configuration of functional modules within the computer apparatus, the method comprising:

storing a module configuration of the computer apparatus, the module configuration being an identification of each functional module in the computer apparatus as validly formed, on a security token removably attachable to the computer apparatus; and

checking an actual module configuration against the stored module configuration;

wherein the computer apparatus contains or is in communication with a trusted device adapted to respond to a user in a trusted manner and the trusted device inhibits function of the computer apparatus if the actual module configuration does not satisfactorily match the stored module configuration.

58. A method as claimed in claim 57, wherein the stored module configuration is stored such that it is accessible only by a cryptographic authentication process.

59. A method as claimed in claim 58, wherein the trusted device is adapted to perform the step of checking the actual module configuration against the stored module configuration.

60. A method as claimed in claim 59, wherein the trusted device is adapted to communicate securely with the security token.

61. A method as claimed in claim 57, wherein the security token is a smart card.

62. A method as claimed in claim 57, wherein the stored module configuration is also held by a remote module validation authority.

63. A method as claimed in claim 62, wherein the step of checking the actual module configuration against the stored module configuration involves use of the stored module configuration held by the remote module validation authority.

64. A method as claimed in claim 62, wherein the remote validation authority provides a service allowing a replacement security token to be provided if a security token is lost or stolen.

65. A method as claimed in claim 44, wherein the trusted device is a tamper-resistant or a tamper-detecting device.

66. Computer apparatus as claimed in claim 52, wherein the trusted device is a tamper-resistant or a tamper-detecting device.

67. A method as claimed in claim 57, wherein the trusted device is a tamper-resistant or a tamper-detecting device.

Evidence Appendix

No evidence is being submitted.

Related Proceedings Appendix

No copies of decisions rendered in related proceedings are being submitted.